

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平5-265867

(43)公開日 平成5年(1993)10月15日

(51)Int.Cl.<sup>5</sup>

G 0 6 F 12/14  
15/78

識別記号

3 2 0 C 9293-5B  
5 1 0 K 7530-5L

庁内整理番号

F I

技術表示箇所

審査請求 未請求 請求項の数2(全 7 頁)

(21)出願番号 特願平4-64424

(22)出願日 平成4年(1992)3月23日

(71)出願人 000004237

日本電気株式会社  
東京都港区芝五丁目7番1号

(72)発明者 岡本 渉

東京都港区芝五丁目7番1号日本電気株式  
会社内

(74)代理人 弁理士 京本 直樹 (外2名)

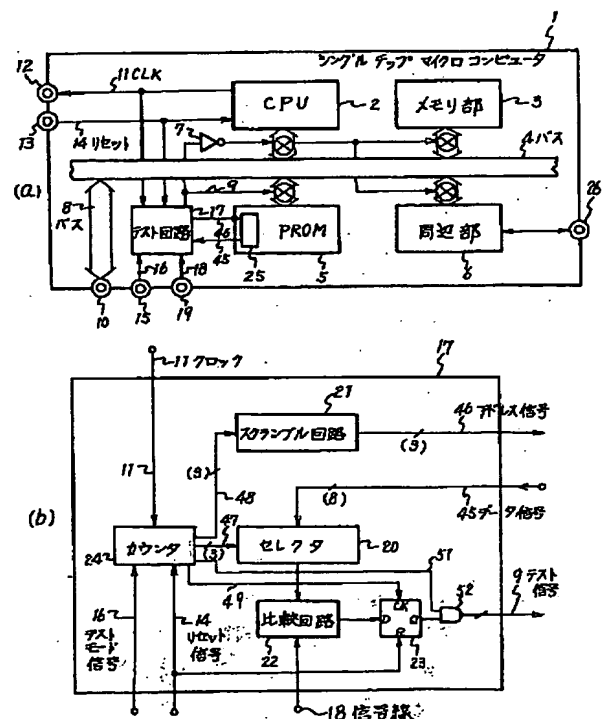
(54)【発明の名称】 シングルチップマイクロコンピュータ

(57)【要約】

【目的】外部からパスワードを入力することによりテストモードを許可し、内蔵PROM格納データを保護する。

【構成】テストモードを許可する回路を、スクランブル回路21、比較回路22、カウンタ24、セレクト20で構成し、外部よりシリアルに信号18によりパスワードを入力すると共に、スクランブル回路21の出力をアドレスとして内蔵PROM5からデータをリードしセレクト20を介して1ビット単位にて比較する。また、カウンタ24にて比較回数を計数し、一定回数に達すると比較を停止させる。比較回路22はPROMの格納データと外部からの入力パスワードを比較し、一致する場合のみ信号9を出力してテストモードを許可する。

【効果】内蔵PROMに格納した秘匿性の高いデータへのアクセスが困難となり、悪用される危険も小さくなる。



(2)

## 【特許請求の範囲】

【請求項1】 単一半導体基板上に中央処理装置、記憶部、周辺部およびプログラマブルROM（以下PROMという）を集積し、このPROMに対しテスト機能を内蔵したシングルチップマイクロコンピュータにおいて、テスト時にクロックを計数するカウンタと、このカウンタの出力アドレスを入替え反転しアドレス信号として出力するスクランブル回路と、前記アドレス信号に対応した前記PROMのデータを前記カウンタの出力により選択するセレクトと、このセレクトの出力と外部から入力したデータ値を比較する比較回路とから構成されるテスト回路を付加し、外部から入力した値と前記PROMの格納値とが等しい場合のみ外部から前記PROMへのアクセスを可能とするようにしたことを特徴とするシングルチップマイクロコンピュータ。

【請求項2】 テスト回路が、PROMの格納値に対するアドレス指定を、このPROMに格納したデータにより行なうものである請求項1記載のシングルチップマイクロコンピュータ。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は、単一半導体基板上にメモリ機能及びコンピュータ機能を集積したシングルチップマイクロコンピュータに関し、特に内蔵PROMに格納した値に対応したデータを外部から入力した場合のみテスト可能としたシングルチップマイクロコンピュータに関する。

## 【0002】

【従来の技術】近年、LSI製造技術の進歩によりシングルチップマイクロコンピュータ（以下シングルチップマイコンという）の分野においても高集積化が進み、単位機能当たりのコストの低下も著しくなっている。

【0003】従来、銀行などの金融機関においては磁気カードが主に使用されてきたが、磁気カードは記憶容量が少なく、またセキュリティの面で問題があり、最近では不正使用、偽造など多くの犯罪が頻発し、大きな社会問題となっている。そこでこの磁気カードに代るものとして、シングルチップマイコンを搭載したICカードが登場し、国内外において実用化に向けて大規模な実験が進んでいる。このICカードは磁気カードに比べて記憶容量も数段大きく、またカード内にコンピュータ機能を内蔵しているのでセキュリティの面でも格段の信頼度がある。

【0004】一般にシングルチップマイコンを搭載したICカードにおいては、データメモリの大部分にUVEPROM (Ultra-Violet Erasable Programmable ROM) またはEEPROM (Electrical Erasable Programmable ROM) を使用しており（以下UVEPROM、EEPROMをPROMという）、そ

のデータメモリをいくつかの領域に分割しそのアクセスを管理している。

【0005】銀行などの金融機関の発行するキャッシュカード、クレジットカードとしてICカードを使用する場合、この分割されたデータメモリの一部をシークレット・ゾーン (Secret Zone) と呼び、銀行の口座番号、IDナンバー、シークレットナンバーなど機密性の高いデータを格納するのに使用している。このシークレット・ゾーンはICカードの不正使用、偽造を防止する上で重要な部分であって、使用時にはソフトウェアによりその領域に対するアクセスを管理し、特別な場合だけ前記領域に対しアクセスできるようになっている。ところが、テストモード時には、容易に外部より内蔵PROMの全領域に直接アクセスが可能であり、シークレット・ゾーン内の値を読み出して悪用したり、故意に変更することが可能であった。

【0006】図6はこの種のシングルチップマイコンの一例のブロック図である。図6において、メモリ部3はユーザプログラム格納及びデータの格納に用いる読出し専用または、読出し書込ともに可能なメモリ、内部バス4はアドレス及びデータを時分割に転送するバス、内部バス8は、テストモード時に、外部端子10を介して内部バス4にアドレス及びデータを転送する際に用いる時分割バスである。

【0007】中央処理装置（以下CPUという）2は、メモリ部3に格納したプログラムに従って、データ処理を行なう。周辺部6は、チップ外部との通信を行なうためのポート等から構成され、内部バス4を介して入力したデータを外部端子26に出力し、外部端子26からデータを入力し、内部バス4に出力する機能を持つ。PROM5は、データメモリとしてUVEPROMまたはEEPROMから構成され、メモリ内にシークレット・ゾーン25を設け、カードのIDナンバー、シークレットナンバー、口座番号等を格納しており、CPUの命令により読出し及び書込みを行なう。このシークレット・ゾーン25へのアクセス管理は、ユーザがソフトウェアにより行なっている。。

【0008】端子15は、テストモード時に「1」とする外部入力端子であり、この時インバータ7の出力が0となるため内部バス4にはPROM5のみ接続され、PROM5へのアクセスがチップ外部より直接可能となる。端子10は、内部バス8を介してアドレス及びデータを外部に入出力する端子であり、内部バス4に接続され、端子12はCPU2の出力するCPUクロック11を出力する端子、端子13はCPU2をリセットする端子で、「1」の時リセット信号14が「1」となりCPU2をリセットする。

【0009】次にテスト時の動作を説明する。端子13を「1」のまま端子15を「1」とし、端子13をCPUクロック11の立下りに同期して0とする。この時、

(3)

3

テスト信号9は「1」となりインバータ7の出力は「0」となるのでCPU2、メモリ部3、周辺部6は内部バス4から電氣的に切離される。従って、内部バス4に接続されているのはPROM5のみとなる。この状態で外部端子10、内部バス8を介してアドレス及びデータをPROM5に入力し、データの読出し及び書込みを行なう。この時、シークレットゾーン25のアドレスを入力すれば容易にゾーン内データにアクセス可能である。従って、データリード及びライトが容易に行なえることとなる。

【0010】以上述べたように従来のシングルチップマイコンにおいては、秘匿データを格納するシークレット・ゾーンに対するアクセス管理をすべてユーザーのソフトウェアにより行なっている。このようなシングルチップマイコンをカードに搭載した場合、テストモードを使用することにより、シークレット・ゾーンに対し不当なデータアクセスを行なうことが可能である。さらにデータメモリに電気消去型読み出し専用メモリ（EEPROM）が使用されている場合には、書込み命令が実行されるとPROM内部で自動的に書込み用の電圧が生成されるので、シークレット・ゾーンに対し、不当な書込みが容易に行なうことが可能である。

#### 【0011】

【発明が解決しようとする課題】上述したように従来のデータメモリにおいて、アクセス保護の領域であるシークレット・ゾーンへのアクセスを管理しているシングルチップマイコンにおいては、内蔵PROMへのアクセス管理をすべてソフトウェアによって行なっているため、テストモード時に容易にアクセス可能であり、不正なアクセスが行われてシークレット・ゾーン内のデータが悪用されたり、また故意にデータが書き換えられる危険性が在るという欠点が存在した。

【0012】本発明の目的は、簡単なテスト回路を付加することにより、テストモード時の不当なアクセスを排除し、より確実なセキュリティが容易に得られるようにしたシングルチップマイコンを提供することにある。

#### 【0013】

【課題を解決するための手段】本発明の構成は、単一半導体基板上に中央処理装置、記憶部、周辺部およびプログラマブルROM（以下PROMという）を集積し、このPROMに対しテスト機能を内蔵したシングルチップマイクロコンピュータにおいて、テスト時にクロックを計数するカウンタと、このカウンタの出力アドレスを入替反転しアドレス信号として出力するスクランブル回路と、前記アドレス信号に対応した前記PROMのデータを前記カウンタの出力により選択するセレクタと、このセレクタの出力と外部から入力したデータ値を比較する比較回路とから構成されるテスト回路を付加し、外部から入力した値と前記PROMの格納値とが等しい場合のみ外部から前記PROMへのアクセスを可能とするよ

4

うにしたことを特徴とする。

#### 【0014】

【実施例】図1（a）、（b）は本発明の第1の実施例のシングルチップマイコンのブロック図およびそのテスト回路17のブロック図である。本実施例においては、新たに追加したテスト回路17以外の構成要素は、図6の従来例と相違がない。従ってテスト回路17を中心に説明する。

【0015】図において、テスト回路17は、CPUの出力するクロック信号11に同期して外部端子19よりシリアルにデータを入力し、PROM5内のシークレットゾーン25に格納した値と外部より入力した、ビットシリアルデータ値を比較して、一致する場合のみテストモードを許可する機能を有する。

【0016】本実施例のテスト回路17は、図1（b）のように、ラッチ回路23、スクランブル回路21、比較回路22、カウンタ24、2入力ANDゲート52から構成される。スクランブル回路21は、カウンタ24の出力するPROMアドレス48をスクランブルし、PROM5に対しアドレス信号46を出力する。セレクタ20は、カウンタ24の出力するセレクト信号47に従って、入力データから1ビットをセレクトし比較回路22に対して出力する。比較回路22は、セレクタ20の出力と、外部からの入力データ18を比較し、一致した時に「1」を、一致しない時は「0」をラッチ回路23に対して出力する。

【0017】カウンタ24は、リセット信号14の立下りに同期してカウントデータをロードし、基本クロック11の立上りに同期し、テストモード信号16が「1」で、リセット信号14が「0」の時のみ、CPUクロック11をダウンカウントする。ラッチ回路23は、カウンタ24の出力するカウント信号49の立下り同期で比較回路22の出力をラッチし、ANDゲート52に対して出力する。また、リセット信号14が「1」の時「0」にクリアされる。ラッチ回路23は、リセット信号14が「0」の時「1」をラッチ後「0」をラッチすると、以後リセット信号14が再度「1」になるまで「0」を保持する。ANDゲート52は、ラッチ回路23の出力とカウンタ24の出力する制御信号51を入力とし、AND出力をテスト信号9として出力する。

【0018】以下、テスト回路17の動作を図2のタイミング図を用いて説明する。まず、リセット信号14を「1」のままテストモード信号16を「0」としておく。次に、テスト信号モード16を「1」とし、リセット信号14をCPUクロック11の立下りに同期して「0」とする。この時、リセット信号14の立下りでラッチ回路23はクリアされる。またカウンタ24は、内蔵のダウンカウンタ及びラッチに初期値をロードする。以下、ダウンカウンタへのロードを「7」、ラッチへのロード値を「3」として説明する。

(4)

5

【0019】CPUクロック11の立上りに同期して外部端子19よりシリアルに8ビットデータを入力する。この時、カウンタ24は、CPUクロック11の立上りに同期して8回カウントする。さらに、カウンタ24のダウンカウンタへの格納値及びラッチの格納値を、各々3ビットのセレクト信号47及び3ビットのPROMアドレスとして出力する。スクランブル回路21は、3ビットのPROMアドレス48をスクランブル（アドレス信号の入替え反転等）し、3ビットのアドレス信号46としてPROM5に対し出力する。カウンタ24内のダウンカウンタは、8回カウント動作後、制御信号51を「1」にして停止する。

【0020】比較回路22は、セクタ20の出力する値と外部から入力する信号18の値が同一の場合「1」をラッチ回路23に対し出力する。また、同一でない場合「0」を出力する。セクタ20は、アドレス信号46にてアドレスしたPROM5の格納データであるデータ信号45に対し、カウンタ24の出力するセレクト信号47で指定する1ビットを選択して出力する。

【0021】従って、本実施例のテスト回路17においては、カウンタ24がダウンカウントしながら出力するセレクト信号47にて選択したPROM5内のデータであるデータ信号45の1ビットと外部からの入力データである信号18を、ビット単位に比較し結果をラッチ回路23にラッチする。そしてダウンカウンタへのロード値にて指定されるビット数（ここでは8）だけ比較し、全ビットが一致した場合のみラッチ回路23の最終値は「1」となる。また、カウンタ24はダウンカウントを終了すると制御信号51に「1」を出力するため、ANDゲート52はテスト信号9に「1」を出力し、テストモードを許可する。

【0022】この比較が、たとえ1ビットでも一致しない場合は、ラッチ回路23の最終値は0となり、テスト信号9が「0」だからテストモードは禁止される。従って、カウンタ24内のダウンカウンタへのロード値+1で指定されるビットのパスワードを外部から入力し、PROM5に内蔵したデータと一致した場合のみテストモードが許可されるため、従来に比べ不正にテストモードを実現することが困難である。さらに、パスワードのビットサイズも可変であり、かつPROM内のパスワード格納値に対するアドレスもスクランブルしてあるので、テストモードによる内蔵PROMへの不正なアクセスはますます困難となる。

【0023】図3は図1のカウント24の構成を示すブロック図である。このカウンタ24は、定数発生回路43、4ビットのダウンカウンタ41、ANDゲート44、3ビットラッチ42から構成される。リセット信号14が「1」の時、ダウンカウンタ41はクリアされて、動作を停止し、ラッチ42もクリアされる。リセット信号14が「0」になると、立下り同期にて定数発生

6

回路43の出力をラッチ42及びダウンカウンタ41の下位3ビットにロードする。また、テストモード信号16が「1」のためダウンカウンタ41はANDゲート44の出力の立上りに同期してカウントダウンし、かつラッチ42の格納値をPROMアドレス47として出力する。また、ダウンカウンタ41はダウンカウントしながらカウンタの下位3ビットの内容をセレクト信号48として出力し、カウンタの動作クロックをカウント信号49として出力する。

【0024】以下、ダウンカウンタ41へのロード値を7として説明する。ダウンカウンタ41は、8回ダウンカウントすると第1〜第4ビットが「1」となるため、ANDゲート44の出力も「0」となり、ダウンカウンタ41はカウント動作を停止する。この時、セレクト信号48は7〜0まで8パターン出力される。従って、データ信号45の全てのビットに対応してセレクト信号48が出力される。

【0025】本実施例においては、簡単なハードウェアから構成されるテスト回路17を付加することにより、第三者によるテストモードの実現が容易でなくなり、シークレット・ゾーン25内のデータに対する不当なアクセスやデータの消失を防ぐことができ、高度なフェール・セーフが実現される。

【0026】図4及び図5は本発明における第2の実施例のシングルチップマイクロコンピュータのテスト回路のブロック図及び図4のカウントのブロック図である。図4のブロック図は図1に対しPROM5からカウンタ24aへのパスが設けられている点でのみ相違している。従って、カウンタ24aの構成及び動作についてのみ述べる。

【0027】本実施例のシングルチップマイコンのカウント24aは、図1のカウント24に対して、ダウンカウンタ41及びラッチ42においてPROM5に内蔵した値を初期ロード値として指定する点で相違する。

【0028】このカウンタ24aは、アドレス「0」のスクランブル値に対応してPROM25より初期値をラッチ42、ダウンカウンタ41にロード後、ダウンカウント動作を行なう。すなわち、第1の実施例と異なり、定数発生回路43の発生するロード値に代って、リセット信号14をハイからロウに変化した時、クリアされたラッチ42の格納値「0」をスクランブル回路21にてスクランブル後アドレス信号46にてアドレス指定し、PROM5からリードしたデータ信号45をロード値として、リセット信号14の立下りにてラッチ42にラッチする。従って、アドレス「0」をスクランブルしたアドレスに格納した値を変更することにより、パスワードの格納アドレスを変更可能であるため、第1の実施例に対しよりセキュリティが高くなる効果がある。

【0029】テスト回路17aは、ラッチ42で指定したPROM5の格納データと外部からの入力データが一

(5)

致した場合のみテスト信号9を出力し、テストモードを実現する。初期値をラッチ42、ダウンカウンタ41にロードして以後の動作は第1の実施例と同様である。

### 【0030】

【発明の効果】以上説明したように本発明においては、内蔵PROMに格納したデータと外部より入力したデータが一致する場合のみテストモードを許可するテスト回路を付加することにより、従来シークレット・ゾーンへのデータアクセスをテストモードの実現にて自由に行なっていた時に生じる不当なデータアクセスを禁止し、高度なセキュリティを実現する効果がある。

### 【図面の簡単な説明】

【図1】(a), (b)は本発明の第1の実施例におけるシングルチップマイクロコンピュータおよびそのテスト回路のブロック図。

【図2】図1のテスト回路の動作を説明するタイミング図。

【図3】図1の実施例のテスト回路内カウンタのブロック図。

【図4】本発明の第2の実施例におけるテスト回路のブロック図。

【図5】図4のテスト回路内のカウンタのブロック図。

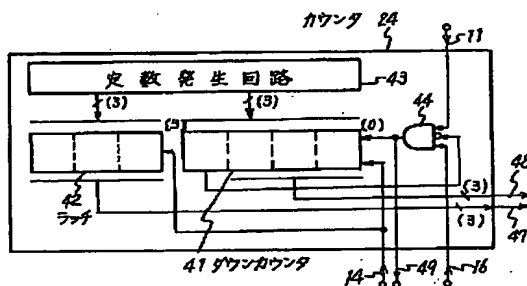
【図6】従来のシングルチップマイクロコンピュータの一例のブロック図。

### 【符号の説明】

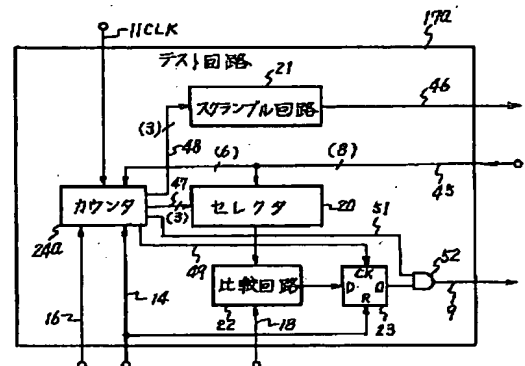
- 1, 1a シングルチップマイクロコンピュータ  
2 CPU  
3 メモリ部

- 4, 8 内部バス  
5 PROM  
6 周辺部  
7 インバータ  
9 テスト信号  
10, ~13, 15, 19, 26 外部端子  
11 CPUクロック  
14 リセット信号  
16 テストモード信号  
17, 17a テスト回路  
18 信号線  
20 セレクタ  
21 スランブル回路  
22 比較回路  
23 ラッチ回路  
24, 24a カウンタ  
25 シークレットゾーン  
41 ダウンカウンタ  
42 ラッチ  
43 定数発生回路  
44, 52 ANDゲート  
45 データ信号  
46 アドレス信号  
47 セレクト信号  
48 PROMアドレス  
49 カウント信号  
51 制御信号

【図3】

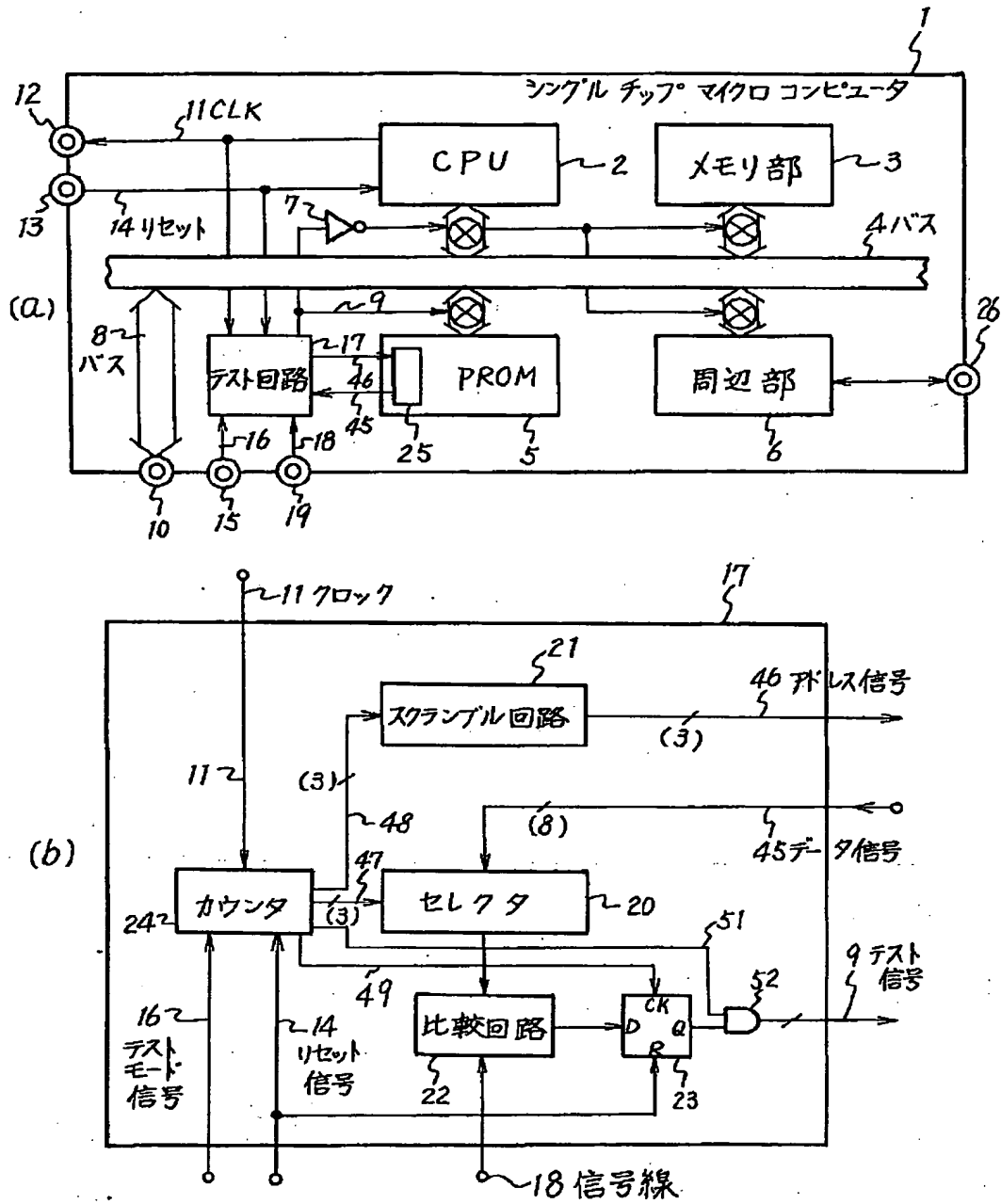


【図4】



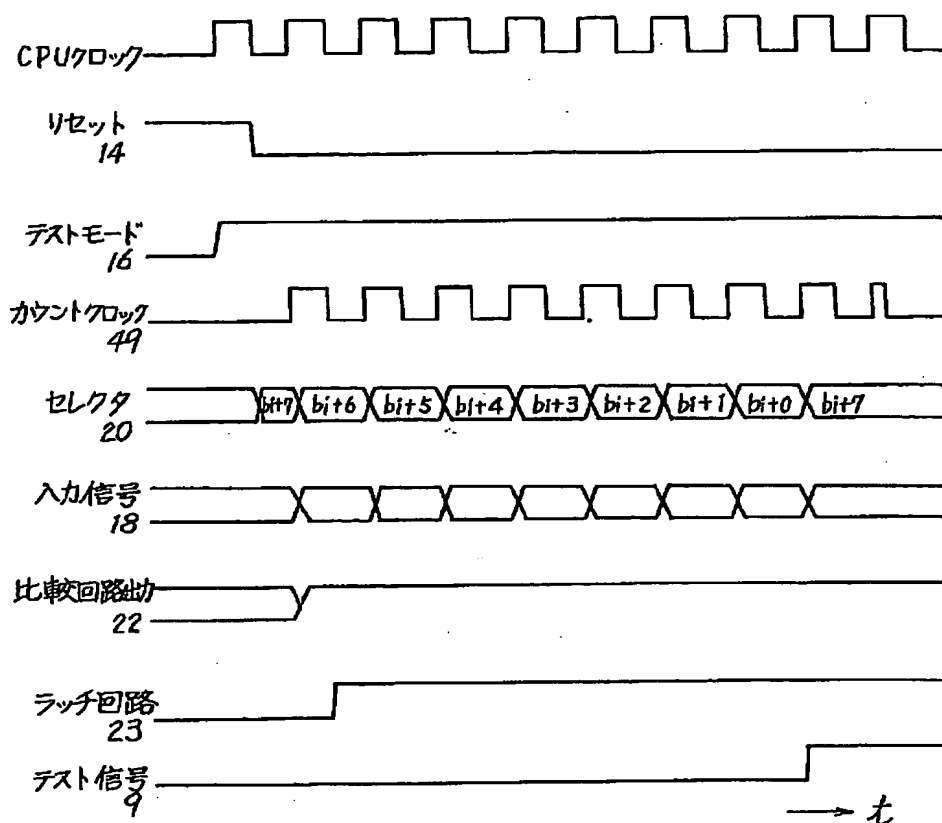
(6)

【図1】

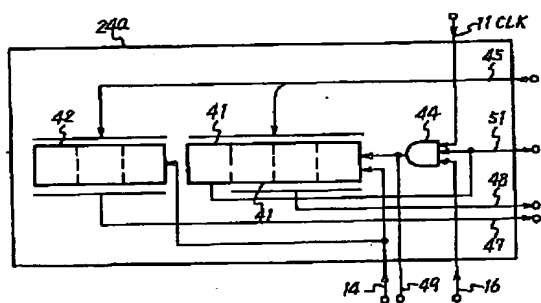


(7)

【図 2】



【圖 5】



【图6】

